汉坤法律评述
2023 年 5 月 14 日

HANKUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

欧盟 AI 法案立法观察

作者：李胜 | 高超星

自 2022 年 11 月 OpenAI 推出其基于 GPT-3.5（Generative Pretrained Transformer，生成型预训练变换模型）系列大模型的聊天机器人应用 ChatGPT 以来，以 AIGC 为代表的 AI 产业迅速在全球范围内掀起新的浪潮，成为最为热门的创业、创新和投资赛道之一。各主要经济体也针对 AI 产业出台了不同的监管政策，我国国家互联网信息办公室于今年 4 月公布了《生成式人工智能服务管理办法（征求意见稿）》并向社会公开征求意见（请参见我们于 2023 年 4 月 12 日推出的文章：***"《生成式人工智能服务管理办法（征求意见稿）》评析"***[1]）；美国商务部下属的国家标准与技术研究院（National Institute of Standards and Technology）于 2023 年 1 月发布了其第一版《人工智能风险管理框架》（AI Risk Management Framework）[2]，拜登政府近期也在其一项行动公告中提出要对现有的生成式人工智能系统进行公开的风险评估[3]；英国政府科学、创新和技术部（Department for Science, Innovation and Technology）也针对人工智能监管发布白皮书，提出人工智能监管的安全性、透明度、问责等监管原则[4]。

在各国 AI 监管立法中，肇始于 2021 年 4 月的欧盟人工智能法案[5]（EU Artificial Intelligence Act，**"欧盟 AI 法案"**或**"法案"**）备受关注。欧盟理事会于 2022 年 12 月 6 日通过了关于该法案的共同立场（Common Position）[6]，欧洲议会内部市场委员会和公民自由委员会于 2023 年 5 月 11 日以压倒性优势通过了该法案的谈判授权草案，该谈判授权草案也是法案的第五个折衷文本[7]（本文主要基于经该折衷文本所修订的法案文本进行分析[8]），并预计于 6 月就该谈判授权草案在欧洲议会层面进行投票表决。该法案有望于 2023 年底正式通过并成为全球首部综合性人工智能监管法律，毫无疑问将对全球的人工智能治理进程产生深远的影响。我们将在本文中对欧盟 AI 法案草案的适用范围、基本思路、监管框架及要点进行分析，以期为各位从业者

[1] https://mp.weixin.qq.com/s/PraizijUn_iuX8OAX_4G1g。

[2] https://www.nist.gov/itl/ai-risk-management-framework。

[3] https://www.whitehouse.gov/ostp/news-updates/2023/05/04/fact-sheet-biden-harris-administration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and-safety/。

[4] https://www.gov.uk/government/news/uk-unveils-world-leading-approach-to-innovation-in-first-artificial-intelligence-white-paper-to-turbocharge-growth。

[5] 在立法过程中，恰逢 AIGC 类产品推出并风靡，欧盟立法者也针对该类产品对法案进行了针对性调整。

[6] https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/。

[7] https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence。

[8] https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf。

和投资人士提供借鉴。

一、规制目标与基本思路

在法案的提出和审议、辩论过程中，欧盟立法者们就法案总体预期目标进行了充分的讨论，其期望通过法案为在欧盟境内开发和使用“值得信赖的人工智能系统”（Trustworthy AI Systems）创造条件，并确保市场的正常运作，其具体的规制目标包括：安全及符合欧盟现有法律、增强法律的确定性和透明度以促进人工智能相关的投资和创新，加强治理并执行符合基本权利及安全要求的人工智能法律，并促进合法、安全和可信的人工智能系统的市场的发展。基于前述规制目标，法案围绕人工智能产品和服务的开发、市场投放及使用明确了一个统一的监管框架，其基本思路为基于风险分析的方法（Risk-based Approach），为不同类型的人工智能系统施加不同的要求和义务，我们将在下文进行具体分析。

二、适用范围

（一）监管对象（Objects）

截至目前，科学界对于“人工智能/Artificial Intelligence”尚未有一个确定的最终定义，而是作为一类计算机应用的统称，故草案基于人工智能系统所使用的技术和方法，就人工智能系统提出了一个较为宽泛且技术中立（Technology-Neutral）的定义：“人工智能系统是指基于机器的系统，它被设计为以不同程度的**自主性**运行，并且可以为了明确或隐含的目标，产生诸如预测、建议或决策等影响物理或虚拟环境的输出”。对于产业参与者来说，其软件系统是否具有自主性元素（在立法者的相关说明中，指人工智能系统在没有人类参与的情况下运行的程度）将成为该系统是否被纳入监管的主要标准。

相比欧盟 AI 法案，我国并未制定一部针对人工智能的统一监管规则，也没有对人工智能的系统性定义，而是通过《互联网信息服务深度合成管理规定》《互联网信息服务算法推荐管理规定》《生成式人工智能服务管理办法》等多部法规的相互衔接，针对不同的细分业态进行分别立法和监管，涉及的监管对象包括深度合成技术[9]、生成式人工智能技术[10]和算法推荐技术[11]等，但从该等监管对象的定义上并未进行明确区分，而是既有交叉，又有各自的特殊性，在适用时可能存在竞合。

（二）监管范围（Scope）

相比于法案的之前几个版本，关键委员会审议通过的折衷文本对于法案的适用对象也进行了较为实质的调整，调整后法案将主要监管人工智能系统的**“提供者（Provider）”**（即开发人工智能系统并将其以自身名义/商标投入市场或投入使用的个人、法人、公共当局、机构或其他主体，且不论其产品是否收费）和**“部署者（Deployer）”**（指任何经过授权使用人工智能系统的个人、法人、公共当局、机构或其他主体，但经授权在非专业活动中使用人工智能系统的个人除外）。这两个定义的范围都非常广泛，只要是提供人工智能服务的主体，无论是开发、发行、还是仅仅作为经销商或中间授权方，都属于监管的对象。此外，该法案具有**广泛的管辖（包括域外适用）范围**，包括属人、属地和实质判断多个管辖标准。法案明确，“提供者”和“部署者”的下列活动均会受到监管：

[9] 深度合成技术，是指利用深度学习、虚拟现实等生成合成类算法制作文本、图像、音频、视频、虚拟场景等网络信息的技术，包括但不限于篇章生成、文本转语音、音乐生成、人脸生成、图像生成，以及三维重建、数字仿真等生成或者编辑数字人物、虚拟场景的技术。

[10] 生成式人工智能，是指基于算法、模型、规则生成文本、图片、声音、视频、代码等内容的技术。

[11] 算法推荐技术，是指利用生成合成类、个性化推送类、排序精选类、检索过滤类、调度决策类等算法技术向用户提供信息。

- 将人工智能系统投入欧盟市场或在欧盟域内投入使用的提供者，而无论该提供者设立于欧盟境内或是第三国；
- 在欧盟境内设立机构或位于欧盟境内的人工智能系统的部署者；
- 但即使提供者或部署者设立于或位于第三国，只要其使用人工智能系统输出的内容在欧盟境内使用，或任一欧盟成员国的法律根据国际公法规则对其适用，那么其也将适用欧盟 AI 法案。在该等情形下，法案还进一步细化明确：虽提供禁止类人工智能系统的提供者不向欧盟境内提供服务，如其在欧盟内设有机构或位于欧盟内，也适用该法案；只要提供者在欧盟境内有进口商、分销商或授权代表，就适用该法案；以及如果位于欧盟的人士因使用在欧盟上市或投入使用的 AI 系统而在健康、安全或基本权利方面受到不利影响，相关主体也受到欧盟 AI 法案的管辖。

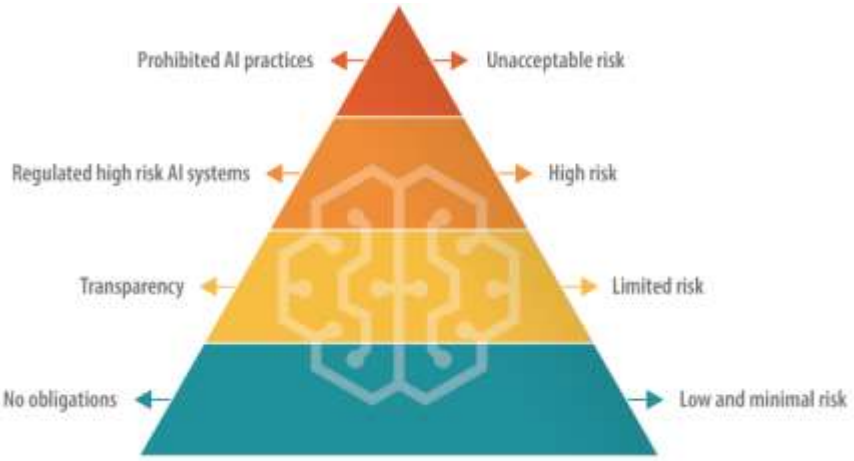
类似于 GDPR，欧洲的监管者们依然采用了坚定的长臂管辖的立场。如果法案最终采用了上述的管辖规范，**对于人工智能系统的产业参与者而言，只要其针对欧盟市场提供产品或开展服务，或其产品的输出物有可能在欧盟境内被销售、使用，甚至位于欧盟的用户可能因使用其产品受到不利影响，就很有可能需要遵守欧盟 AI 法案的相关规定。根据欧盟 AI 法案的要求进行合规运营，将会是每个希望开展国际化运营的 AI 创业者不得不面对的课题。**

相比欧盟 AI 法案，我国针对人工智能监管的三部主要法规在适用范围上采取了不同的界定方法，《互联网信息服务深度合成管理规定》《互联网信息服务算法推荐管理规定》强调法规适用对象为“在中国境内提供”相关服务，《生成式人工智能服务管理办法（征求意见稿）》则强调“面向境内公众提供”相关服务，但结合相关法规的文义和立法目的，该等法规预期的目的仍然是只要相关人工智能服务可以在中国境内被使用，均应适用该等法规的要求，而不论服务提供者是否位于中国境内。但按照《生成式人工智能服务管理办法（征求意见稿）》的语义解读，如果一个中国的企业开发了一款面向中国境外的生成式人工智能产品，则不受该法规限制。

三、基于风险的监管框架及提供者的义务

欧盟 AI 法案基于风险识别的方法，针对不同类型的人工智能系统量身定制了相应的监管措施，其主要区分了不可接受的风险、高风险、有限风险和低或轻微风险四种风险类型，并针对不同类型施加了不同的监管措施以及相应类型的人工智能系统的提供者义务。基于前述风险识别的方法，人工智能系统将仅在解决特定风险水平的严格必要情况下进行监管。欧盟 AI 法案的监管框架呈现出如下特征：

（一）基于风险识别的监管体系（Risk-based Approach）



“人工智能软件风险金字塔模型”，来源：https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

风险类型	人工智能系统的特征	核心监管措施
不可接受的风险	■ 部署超出人的意识的潜意识技术或者故意操作性或欺骗性技术，通过明显削弱个人做出知情决定的能力来严重扭曲用户行为，并对其导致或可能导致伤害的人工智能系统； ■ 利用特定人或特定群体的弱点（如人格特征、社会或经济状况、年龄、身体或心理特征），实质扭曲用户行为，并对其导致或可能导致伤害的人工智能系统，包括根据敏感或受保护的属性或特征或基于对这些属性或特征的推断对自然人进行分类的生物识别分类系统； ■ 对自然人用于社会性评价或分类目的且将给与其不公平待遇的人工智能系统； ■ 预测性警务系统（基于特征分析、位置或过去的犯罪行为）； ■ 通过从互联网或闭路电视无针对性地抓取面部图像来创建或扩展面部识别数据库的人工智能系统； ■ 在执法、边境管理、工作场所和教育机构中推断自然人情绪的人工智能系统	禁止投放市场、投入服务或在欧盟境内使用
高风险	高风险人工智能系统系指对人类的安全及基本权利产生负面影响的人工智能系统，包括： ■ 属于欧盟健康和安全协调指令项下的类型（如玩具、航空、汽车、医疗设备、电梯）且根据前述协调指令需要进行第三方合格评估的产品； ■ 拟作为上述（i）中的产品的安全部件且被要求接受第三方合格评估的产品；	法案对高风险人工智能系统的提供者和部署者施加了一系列义务，以控制AI 系统的风险，核心义务包括下述： ■ **建立充分的风险管理系统**：该系统应涵盖人工智能系统的全生命周期，并进行定期更新，以识别、分析、消除、缓解或控制对健康、安

风险类型	人工智能系统的特征	核心监管措施
	■ 应用于以下领域的人工智能系统（且该等系统将对健康、安全、环境或基本权利构成重大风险，是否构成重大风险的判断标准将由欧洲人工智能委员会（**“委员会”**，由成员国和欧盟委员会代表组成，负责法案的实施）另行制定指导方针）： (1) 自然人的生物识别和分类； (2) 关键基础设施的管理和运作； (3) 教育和职业培训； (4) 就业、人员管理及自营职业的获取等人力资源决策； (5) 评估个人获得和享受基本的公共服务及福利的资格； (6) 干扰基本权利的执法； (7) 移民、庇护和边境管理制度； (8) 司法管理和裁决。 除上述列举的高风险清单外，委员会也获得了一项授权，如其认为一项人工智能系统对健康、安全及基本权利造成不利影响的可能性和严重程度已经相当于或大于上述明确列举的领域，则其可以扩充这一清单	全和基本权利存在的风险，且该风险管理系统应当进行事先测试； ■ **应使用高质量训练、验证和测试的数据集**（针对利用数据训练模式的系统）：且相关的数据训练、验证和测试应当符合数据处理者对数据进行选择、收集、处理、制定相关假设、评估可用性、数量和适宜性、对歧视、偏见信息的审查以及确定数据缺乏性等流程，并遵守欧盟的数据立法，包括但不限于对个人数据进行保护、加密等措施； ■ **建立质量管理体系：**根据法案的要求建立质量管理体系，包括合规战略、对于系统的涉及、控制和验证技术、系统开发、质量控制的行动等等； ■ **准备反映 AI 系统的所有必要信息和目的及合规性的技术文件**：主要目的是为了向主管机关提供必要信息以供风险评估，该等文件包括对 AI 系统的概括性描述，对其要素和开发过程的详细描述，关于 AI 系统的检测、运作和控制的详细资料，对风险管理系统的描述，对 AI 系统在其生命周期内所作的任何改变的说明，适用欧洲协调立法项下的标准的清单，合规声明，上市后阶段系统性能评估的描述等； ■ **记录保存**：AI 系统应具备开发日志自动记录能力，以便自动记录，确保 AI 系统运作的可追踪性； ■ **透明度及信息提供义务**：应向用户提供关于 AI 系统操作的适当透明度和清楚的信息，包括提供者的身份信息、系统特点和能力、预期目的、准确性水平、监督措施、所需的硬件资源相关风险等； ■ **人类监管**：确保人类对于 AI 系统在使用时的有效监管，包括提供者

风险类型	人工智能系统的特征	核心监管措施
		和用户可以采取的监管措施，包括监督系统运作，认识到系统的“自动化偏见”，对系统的输出进行正确解释，在特定情况下拒绝使用系统输出，干预（如终止）系统运行等； ■ **准确度、稳健性和网络安全**：提供者需要表明系统的准确度水平，以技术冗余方法确保稳健性，且开发方式尽可能地消除或减少可能有偏见的输出影响未来操作的输入的风险等
有限风险	■ **与人类互动的系统（如聊天机器人）**； ■ 情感识别系统； ■ 生物识别分类系统； ■ **生成或操纵图像、音频、视频等内容（如深度伪造）的人工智能系统**	仅需遵守透明度义务（即 AI 系统应允许适当的可追溯性和可解释性，同时让人类意识到他们与 AI 系统进行通信或交互，并及时告知用户该 AI 系统的能力和局限性以及受影响的人关于他们的权利）
低或轻微风险	除上述系统之外的人工智能系统	无义务或特殊监管规则

（二）高风险人工智能系统重点监管

欧盟监管的重点在于上述的**高风险人工智能系统**，为了确保上表所述的监管政策能够落到实处，法案也提出了登记注册要求，即所有高风险系统的提供者在将其产品投入市场或投入使用前，应当在欧盟范围内由委员会建立和管理的数据库进行注册。高风险人工智能系统在使用“CE”标识（即安全合格标志）并投入市场或投入使用前，均应当遵守现有产品安全法规的相关要求（如医疗器械类产品应遵守医疗器械相关立法的要求）；如属于目前没有受到欧盟现有产品安全法规管辖的人工智能系统，应当自行进行合格性评估，且评估结果应符合上述对于高风险系统的要求；特别地，对于用于生物识别的高风险人工智能系统，则需要由欧盟认证机构（Notified Body，法案规定每个成员国至少应指定一个认证机构，负责评估程序的执行和对相关主体的监督）进行评估，方可投入市场。

除对于人工智能系统的一般性事前评估要求外，法案也对 AI 产业链的不同参与者也提出了细化的要求：

- **提供者是 AI 系统的最终负责人：**除确保人工智能系统符合上述表格中的相关要求外，还应当遵守一系列义务，包括：在人工智能系统上标明其名称、注册商标、联系地址等信息；建立完善的质量管理系统；在其系统投放到市场或投入使用后的 10 年内，保留相关的技术文件、质量管理文件、评估文件、合规声明等并有义务将该等文件提交监管；保留系统生成的日志；履行数据库登记义务；就不合规定的系统进行整改等等。需要注意的是，只要相关主体把自己的名称、商标放在高风险人工智能系统、或对已投放的人工智能系统进行重大修改，或修改其使用目的，或将人工智能系

统的一个组成部分投放市场或投入使用的主体，均构成提供者而需要遵守相关的义务。**因此，基于开源的人工智能大模型开发产品并提供服务的主体，应同样遵守提供者的相关义务。**

- **部署者要履行风险防范义务：**即采取适当的技术措施（如人类监督、定期检测网络安全措施等），确保人工智能系统被合规使用，并且在将高风险人工智能系统投入使用前，应当在具体使用环境中对系统的影响进行评估。

- **其他参与者要履行以审查义务为核心的一系列的合规义务：**如对于进口商而言，其在进口相关 AI 系统前，应确保其符合评估程序、已制定技术文件，有安全合格证等；对于分销商而言，其审查义务包括核实相关 AI 系统是否带有 CE 标志，是否具有合规性声明及使用说明文件等。

（三）有限风险和低风险系统有较高自由度

不同于高风险人工智能系统因可能会对人类的安全、健康及基本权利造成不利影响而受到强监管，有限风险和低或轻微风险的人工智能系统在法案框架下有较高的自由度。对于**与人类互动的人工智能系统**（典型代表就是各类聊天机器人），提供者只需要确认使用者知悉其正在与 AI 对话即可（即应明确告知消费者），同样的义务也适用于**生物识别分类系统**（根据自然人的生物特征数据将其划分为特定类别的人工智能系统）、**情感识别系统**（指以自然人的生物识别数据为基础，识别或推断其心理状态、情感或意图的人工智能系统）以及**深度合成系统**（如 Deepfake）。不过，法案也明确提出不限制各成员国针对前述人工智能系统制定进一步的透明度规则。

根据目前法案草案对于人工智能系统的风险界定，一些目前人工智能领域比较活跃的产品，如聊天机器人、文字和图片识别及生成软件、AI 伴侣等类型的应用大多属于有限风险和低或轻微风险的人工智能系统，只需保证在透明度规则基础上运营即可，而无需取得特殊的牌照、认证或履行繁杂的报告、监督、记录留存等义务。**但从事 AI 相关业务的企业，仍需要在法案正式通过后，结合法案的最终规定，在日常运营中关注其产品是否构成收到特殊监管的产品（如汽车领域的自动驾驶相关的人工智能、医疗领域的 AI 软件等均应重点关注）或涉及其他特殊领域而构成“高风险人工智能系统”，或属于非为特定目的、特定领域设计的“通用型人工智能”。**

（四）通用型人工智能（General Purpose AI System）和基础模型（Foundation Model）的特别监管措施

在法案进行审议、修订的过程中，以 GPT-3、DALL-E、Midjourney 等通用模型为代表的通用型人工智能的风靡也同样引起了立法者的关注，故在草案中也同样引入对“**通用型人工智能系统**”的特别监管措施。通用型人工智能是指非为特殊目的进行特别设计的具有广泛适用性的人工智能系统，其一般功能包括但不限于图像和语音识别、音频和视频生成、模式检测、问答、翻译和其他功能。一个人工智能系统是否构成通用型人工智能系统，并不以该系统投入市场或使用的方式作为判断标准，**开源软件、作为预训练模型进行发布等类型的系统同样构成受监管的通用型人工智能系统**，通用型人工智能系统可以在多个语境下使用，并且可以集成在其他人工智能系统中。法案对于通用型人工智能系统提出了特别要求，包括：

- 能被用于（**而不论是否实际被用于**）高风险人工智能系统或其组件的通用型人工智能系统应当适用高风险人工智能系统的监管规则；

- 符合上述（i）的特点的通用型人工智能系统的提供者应当遵守高风险人工智能系统的提供者的相关义务，并履行相关的内部控制和合格性评估程序；

- 该类系统的提供者应当在系统投放到欧盟市场的 10 年内保留相关的而技术文件并提供给监管部门；
- 通用型人工智能系统的提供者应当与将通用型人工智能系统用于高风险领域的主体进行适当合作并提供必要信息（知识产权信息和商业机密信息除外）。

虽然上述对于通用型人工智能系统的要求比较严苛，但提供者可以自主选择在其系统中声明相关系统不应被适用于高风险用途（且在其发现系统被滥用时应采取措施加以阻止），以排除上述要求的适用。除上述规定外，法案对于通用型人工智能，特别是基础模型的监管还有可能更进一步，根据欧洲议会成员近期达成的一份临时政治协议[12]，法案对通用型人工智能、特别是基础模型施加更为严格的义务。基础模型是指在广泛的数据上进行规模化训练，为输出的通用性而设计，并可适应广泛的独特任务的人工智能系统模型；其核心特点在于**为非预期的目的而设计，且经过大量的数据训练，具有很强的可适应性**，无论该等基础模型是作为独立模型提供，还是嵌入其他人工智能系统或产品中，或作为通过应用程序接口（API）、开源许可软件使用或通过其他渠道等分发，典型代表如 GPT 模型、Stable Diffusion 模型等。）法案要求基础模型应该与高风险系统一样，在欧盟数据库中进行注册，此外，还需要遵守包括下述在内的额外义务：

- 通过适当的涉及、测试和分析等证明其产品对于健康、安全、基本权利、环境、民主、法治的风险的减少，包括但不限于引入独立专家的参与；
- 在其模型中只纳入受适当数据管理措施约束的数据集，检查数据来源的可持续性、可能的偏差及采取相应的缓解措施；
- 在其全生命周期保持适当的性能、可解释性、可更正性、安全性；
- 遵守适用的标准以减少能源使用、资源使用和浪费，提高资源利用和系统的整体效率；
- 制定详细的技术文件和易懂的使用说明，使下游供应商能够合规使用；特别是通过提供 API 进行服务的基础模型，应当在其提供服务的过程中与下游供应商合作，以控制相关的风险；
- 建立质量管理体系。

需要特别关注的是，对于 AIGC 类型的基础模型（指专门用于生成复杂文本、图像、音频或视频内容的人工智能系统的基础模型）的系统提供者，以及将基础模型用于 AIGC 的系统提供者，法案还提出了额外的要求，包括遵守特定的透明度义务；在可行的情况下对基础模型进行训练，以使其不会产生违反欧盟法律的内容，不损害基本权利及表达自由。此外，在不影响相应国家及欧盟版权法的情况下，还需要记录并公开提供受版权法保护的训练数据的使用情况的详细摘要。

（五）严格的惩罚措施

在法案项下，除委员会负责促进法案的实施并协调各成员国监督机构之间的合作外，各成员国的市场监督机构将实际负责对于高风险人工智能系统合规情况的监督，并有权要求系统提供者针对不合规的人工智能系统采取纠正措施，甚至**禁止、限制、撤销或召回**不符合法案要求的人工智能系统，成员国的监督机构也有一定的自由裁量权，包括对虽然符合法案要求但对人的健康或安全或基本权利或其他公共利益保护构成风险的人工智能系统采取必要相应的监管措施。根据违法行为的严重程度，法案规定

[12] https://www.euractiv.com/section/artificial-intelligence/news/ai-act-meps-close-in-on-rules-for-general-purpose-ai-foundation-models/。

了不同规模的行政罚款以制裁不遵守法案的行为：如对于不遵守禁止性人工智能系统相关规定的主体，将被处以最高 4,000 万欧元或者违法者全球年营收总额 7%的罚款；不遵守高风险人工智能系统项下数据集训练质量以及就人工智能系统进行明确说明的主体，将被处以最高可达 2,000 万欧元或违法者全球年总营业额的 4%的处罚；未遵守法案的其他规定（包括对于基础模型的规定）的主体，则将会被处以最高可达 1,000 万欧元或违法者全球年总营业额的 2%的处罚等。

四、评价与展望

与我国在人工智能领域针对不同的互联网业态进行动态监管并适时回应实践需求、规范行业发展的监管思路不同，欧洲立法者希望为人工智能领域的规范发展建立一个完整、系统的监管框架，但人工智能（特别是 AIGC）近年来的快速发展和更新迭代，为法案预期目标的实现带来了不小的挑战，法案在审议过程中的争论以及法案推进到后期时对于通用型人工智能和基础模型的紧急“打补丁式”的修补均印证了这一点。欧盟 AI 法案的立法目标核心在于减少人工智能风险对于个人健康、安全和基本权利等的风险，对人工智能带来的社会风险则并未进行过多关注，这与我国人工智能领域相关法规强调内容合规及社会影响的监管目标（我国针对人工智能监管的三部主要法规均针对具有社会影响的人工智能技术提出了特别要求，如基于深度合成技术制作的新闻信息要求建立辟谣机制、对具有舆论属性或者社会动员能力的算法推荐服务提供者开展安全评估、AI 生成内容应当真实准确并对违规内容进行过滤和处置等要求）也存在显著不同。

欧盟 AI 法案在其制定过程中也饱受争议，最广泛的批评包括其对监管对象（人工智能系统）的界定过于宽泛而有过度监管之嫌；此外，针对通用型人工智能特别是基础模型的强监管义务也引发了产业界的担忧。正是由于 AI 产业的快速变化和围绕立法产生的争议，法案的进程也非常波折，但外界仍积极预测该法案将于今年年底正式成为法律并于 2 年的缓冲期后开始生效。对于该法案的后续动态，我们也将持续追踪。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

李胜

电话： +86 10 8525 4691
Email： sheng.li@hankunlaw.com